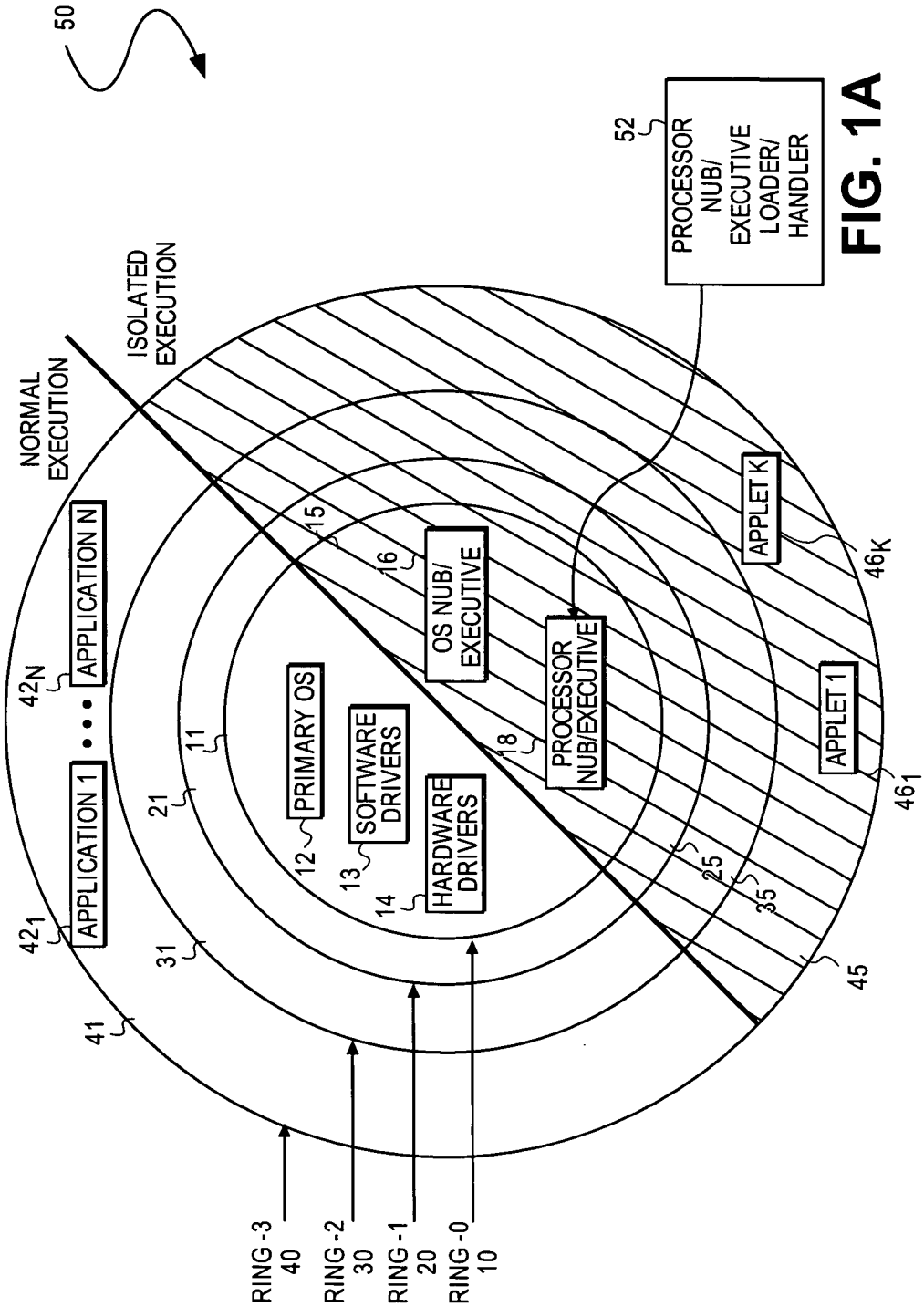


FIG. 1A

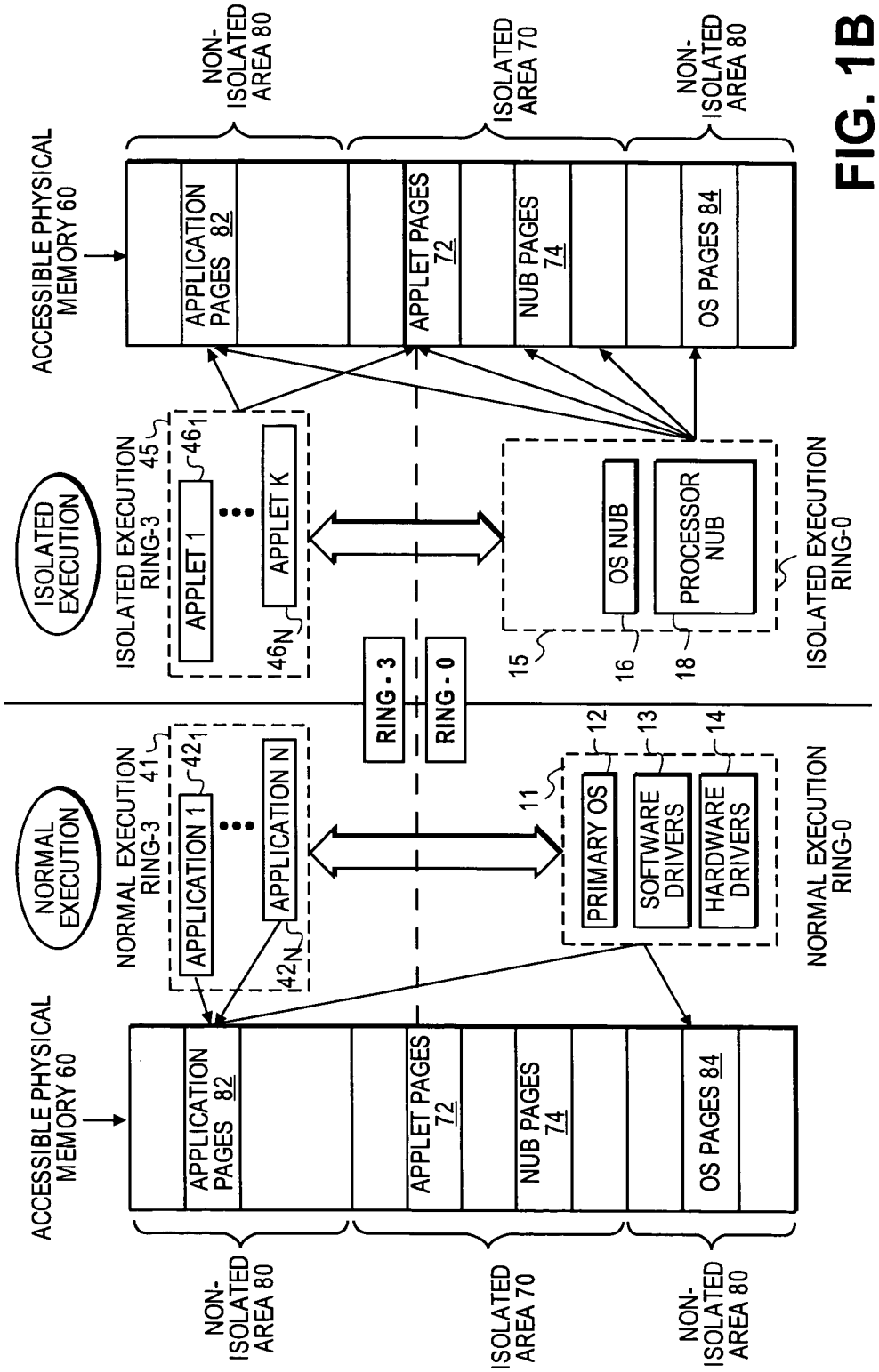

ACCESSIBLE PHYSICAL MEMORY 60
NON-ISOLATED AREA 80
ISOLATED AREA 70
NON-ISOLATED AREA 80
APPLICATION PAGES 82
APPLET PAGES 72
NUB PAGES 74
OS PAGES 84
ISOLATED EXECUTION
ISOLATED EXECUTION RING-3 45
APPLET 1
APPLET K
461
46N
OS NUB
PROCESSOR NUB
ISOLATED EXECUTION RING-0
15
16
18
RING - 3
RING - 0
NORMAL EXECUTION
NORMAL EXECUTION RING-3 41
APPLICATION 1
APPLICATION N
421
42N
11
PRIMARY OS
SOFTWARE DRIVERS
HARDWARE DRIVERS
12
13
14
NORMAL EXECUTION RING-0
ACCESSIBLE PHYSICAL MEMORY 60
APPLICATION PAGES 82
APPLET PAGES 72
NUB PAGES 74
OS PAGES 84
NON-ISOLATED AREA 80
ISOLATED AREA 70
NON-ISOLATED AREA 80

FIG. 1B

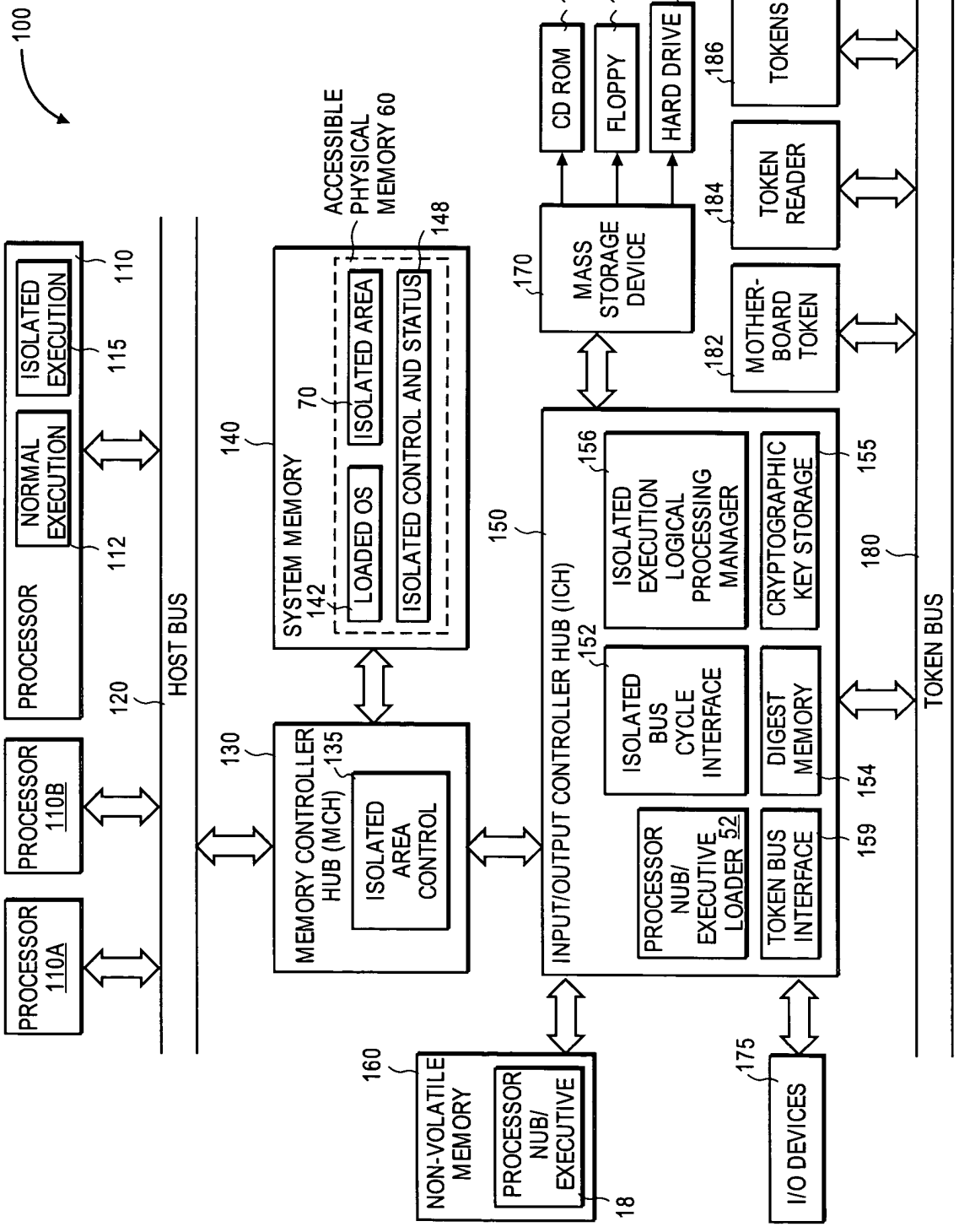

100
PROCESSOR 110A
PROCESSOR 110B
PROCESSOR
NORMAL EXECUTION
ISOLATED EXECUTION
110
115
112
120
HOST BUS
MEMORY CONTROLLER HUB (MCH)
130
135
ISOLATED AREA CONTROL
140
SYSTEM MEMORY
142
LOADED OS
70
ISOLATED AREA
ACCESSIBLE PHYSICAL MEMORY 60
148
ISOLATED CONTROL AND STATUS
150
INPUT/OUTPUT CONTROLLER HUB (ICH)
152
ISOLATED BUS CYCLE INTERFACE
156
ISOLATED EXECUTION LOGICAL PROCESSING MANAGER
155
CRYPTOGRAPHIC KEY STORAGE
180
DIGEST MEMORY
154
PROCESSOR NUB/ EXECUTIVE LOADER 52
TOKEN BUS INTERFACE
159
TOKEN BUS
NON-VOLATILE MEMORY
160
PROCESSOR NUB/ EXECUTIVE
18
I/O DEVICES
175
MASS STORAGE DEVICE
170
CD ROM
172
FLOPPY
174
HARD DRIVE
176
MOTHER-BOARD TOKEN
182
TOKEN READER
184
TOKENS
186

FIG. 1C

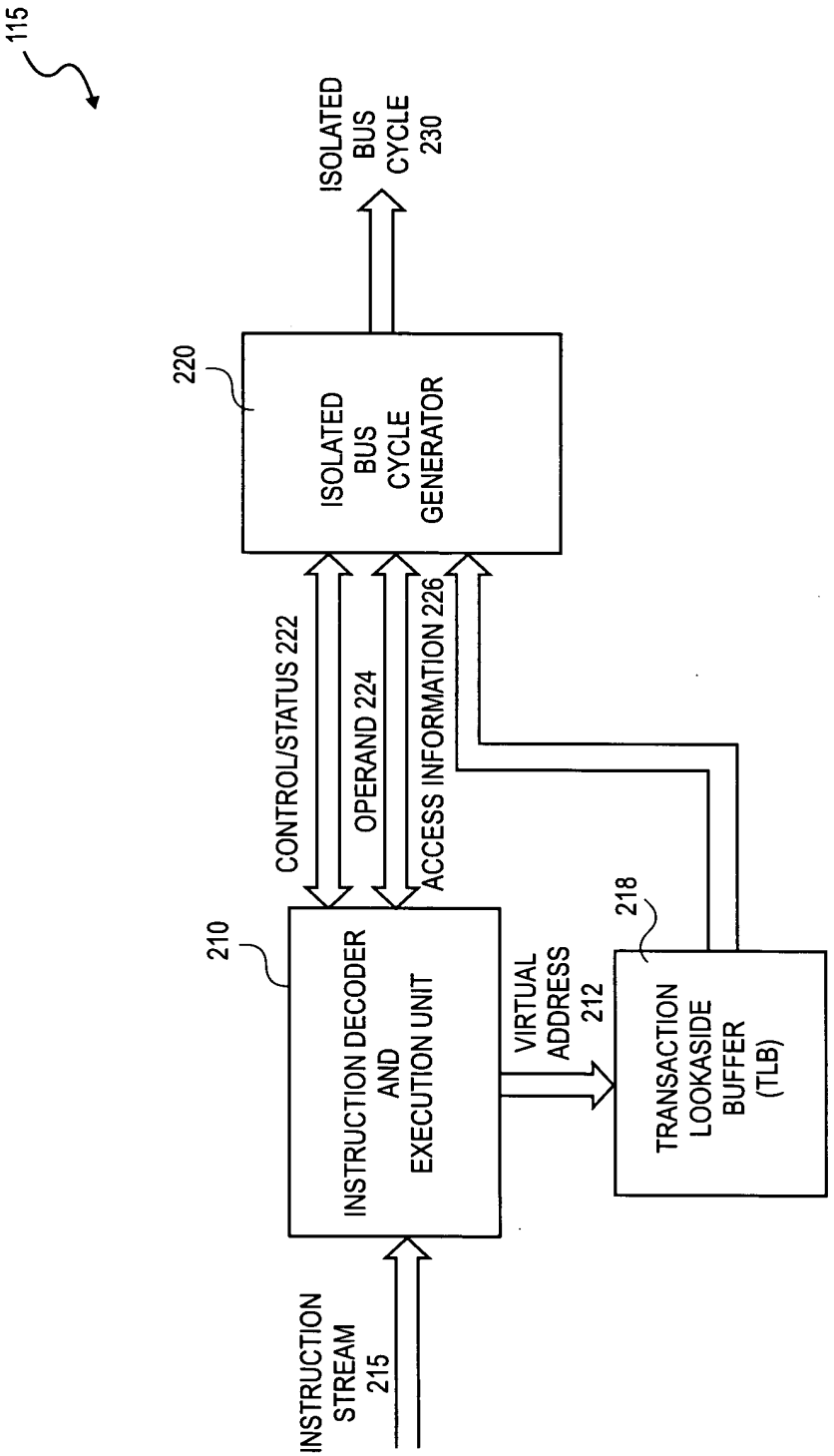

115
ISOLATED BUS CYCLE 230
220
ISOLATED BUS CYCLE GENERATOR
CONTROL/STATUS 222
OPERAND 224
ACCESS INFORMATION 226
210
INSTRUCTION DECODER AND EXECUTION UNIT
VIRTUAL ADDRESS 212
218
TRANSACTION LOOKASIDE BUFFER (TLB)
INSTRUCTION STREAM 215

FIG. 2A

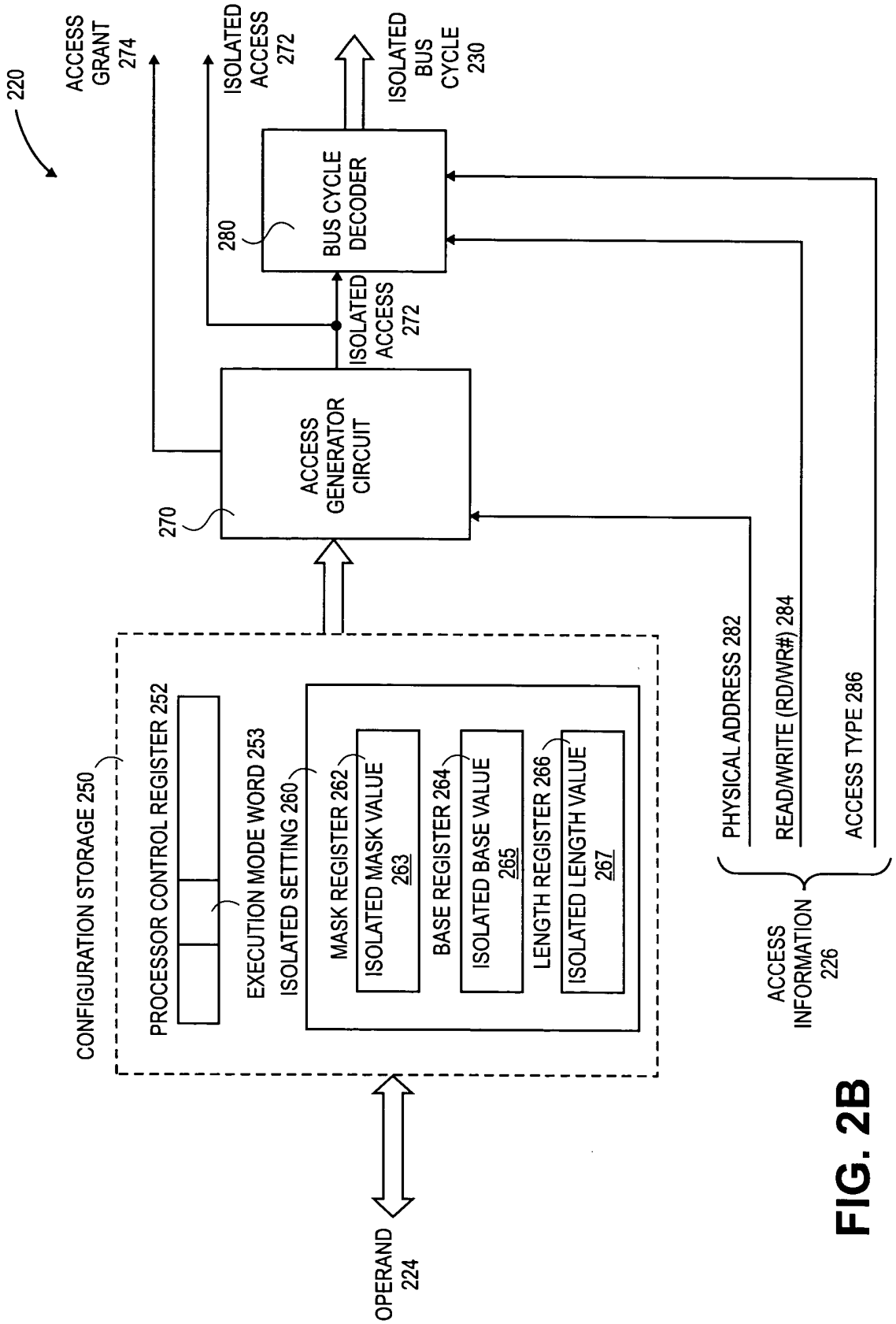

220
ACCESS GRANT 274
ISOLATED ACCESS 272
ISOLATED BUS CYCLE 230
280
BUS CYCLE DECODER
ISOLATED ACCESS 272
ACCESS GENERATOR CIRCUIT
270
CONFIGURATION STORAGE 250
PROCESSOR CONTROL REGISTER 252
EXECUTION MODE WORD 253
ISOLATED SETTING 260
MASK REGISTER 262
ISOLATED MASK VALUE 263
BASE REGISTER 264
ISOLATED BASE VALUE 265
LENGTH REGISTER 266
ISOLATED LENGTH VALUE 267
PHYSICAL ADDRESS 282
READ/WRITE (RD/WR#) 284
ACCESS TYPE 286
ACCESS INFORMATION 226
OPERAND 224

FIG. 2B

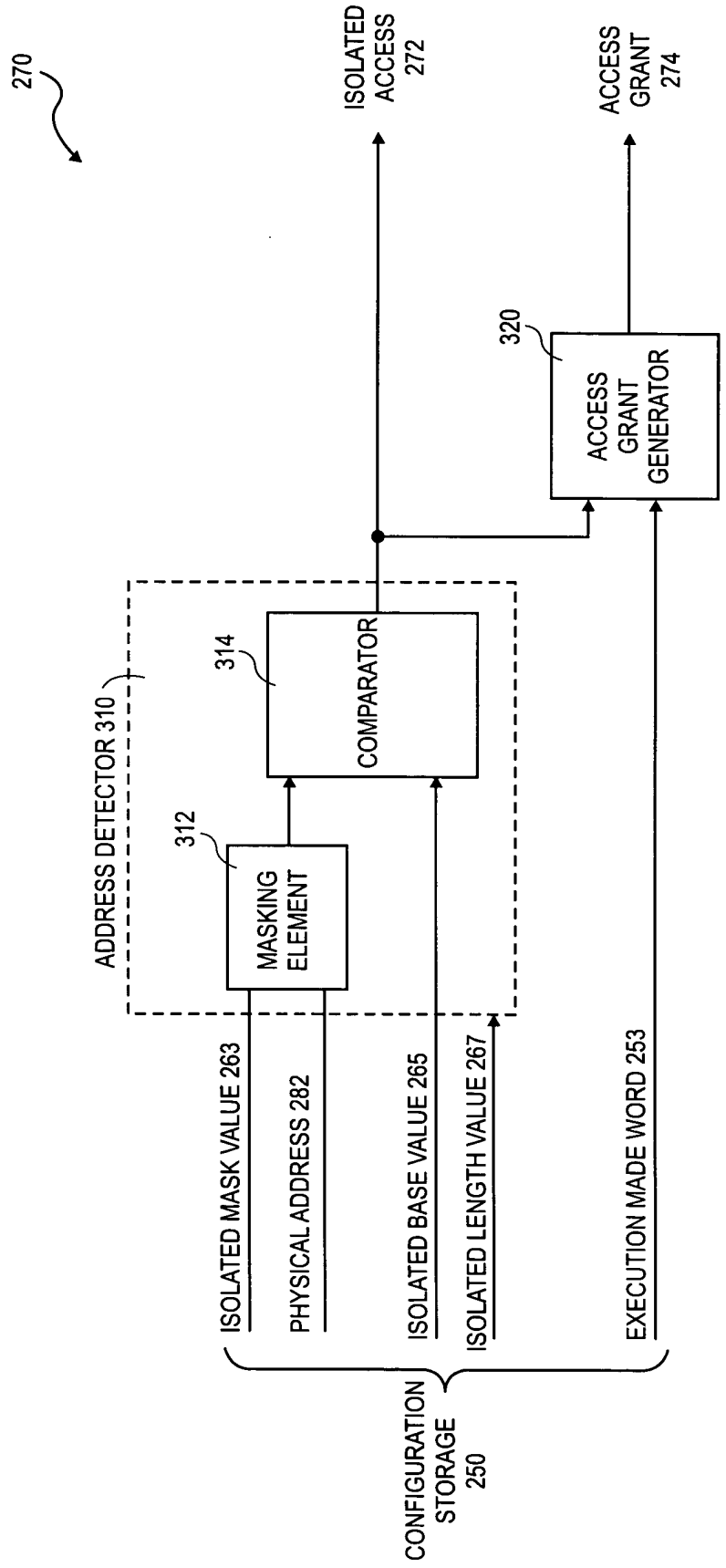
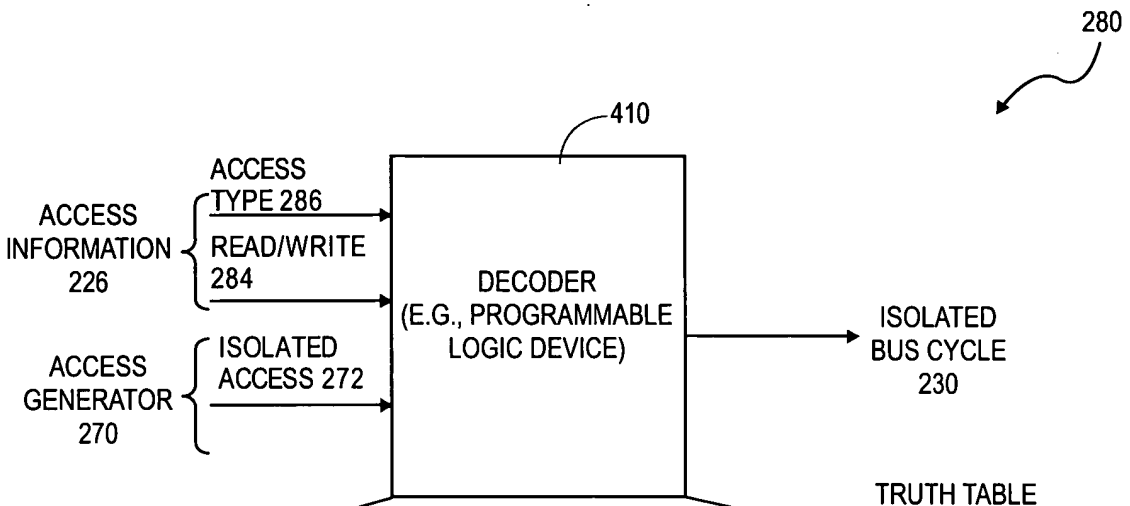

270
ISOLATED ACCESS 272
ACCESS GRANT 274
320
ACCESS GRANT GENERATOR
ADDRESS DETECTOR 310
314
COMPARATOR
312
MASKING ELEMENT
ISOLATED MASK VALUE 263
PHYSICAL ADDRESS 282
ISOLATED BASE VALUE 265
ISOLATED LENGTH VALUE 267
EXECUTION MADE WORD 253
CONFIGURATION STORAGE 250

FIG. 3



ACCESS TYPE		RD/WR#	ISOLATED ACCESS	ISOLATED BUS CYCLE		RING-LEVEL
ISOLATED ENABLED STATE	M/IO#					
X	X	X	DE-ASSERTED	NOT AVAILABLE		0
ENTRY (E.G., ISO_INIT)	X	X	ASSERTED	THREAD ENTRY	THREAD CYCLE	0
WITHDRAW (E.G., ISO_CLOSE)	X	X	ASSERTED	THREAD WITHDRAWAL		0
X	MEMORY REFERENCE	READ	ASSERTED	ISOLATED DATA READ	DATA ACCESS CYCLE	0
X	MEMORY REFERENCE	WRITE	ASSERTED	ISOLATED DATA WRITE		0
X	I/O REFERENCE	READ	ASSERTED	ISOLATED CONTROL READ	CONTROL ACCESS CYCLE	0
X	I/O REFERENCE	WRITE	ASSERTED	ISOLATED CONTROL WRITE		0

FIG. 4

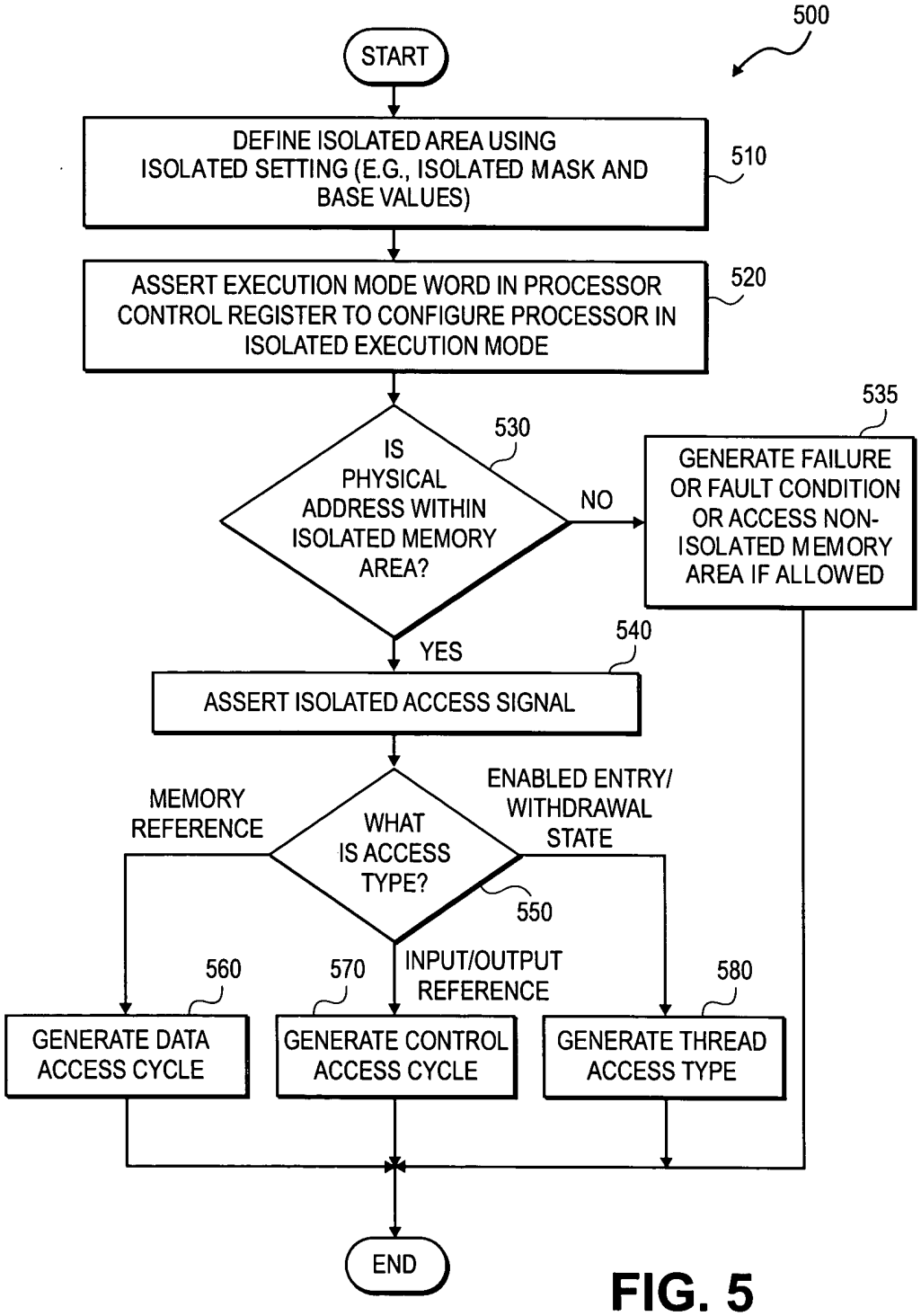

500
START
DEFINE ISOLATED AREA USING ISOLATED SETTING (E.G., ISOLATED MASK AND BASE VALUES)
510
ASSERT EXECUTION MODE WORD IN PROCESSOR CONTROL REGISTER TO CONFIGURE PROCESSOR IN ISOLATED EXECUTION MODE
520
IS PHYSICAL ADDRESS WITHIN ISOLATED MEMORY AREA?
530
NO
GENERATE FAILURE OR FAULT CONDITION OR ACCESS NON-ISOLATED MEMORY AREA IF ALLOWED
535
YES
ASSERT ISOLATED ACCESS SIGNAL
540
WHAT IS ACCESS TYPE?
550
MEMORY REFERENCE
INPUT/OUTPUT REFERENCE
ENABLED ENTRY/ WITHDRAWAL STATE
GENERATE DATA ACCESS CYCLE
560
GENERATE CONTROL ACCESS CYCLE
570
GENERATE THREAD ACCESS TYPE
580
END

FIG. 5